

Appl. No. 09/896,163
Response dated February 2, 2006
Reply to Office Action of November 2, 2005

PATENT

REMARKS/ARGUMENTS

Claims 1-10 and 12-21 were pending. Claims 1-10 and 12-21 were variously rejected under 35 USC 103(a) in light of Yatsukawa in view of Baskey and in view of Chang or Arthan.

I. THE PRESENT INVENTION

Embodiments of the present invention relate to secure computer network access.

As discussed previously, in the various embodiments, the client requests a one-time password from an external server, step 490. In response, the external server provides the one-time password, which is inactive back to the client, steps 500-530. Accordingly, if any one intercepts the one-time password at this stage, and attempts to gain access to the system, because the one-time password is inactive, the access will be denied. Further, because the one-time password is initially determined, and provided in the challenge, the one-time password should be inactive. Otherwise, a client who receives the challenge will be able to gain access to the network using the one-time password, even though she may be unauthorized.

Notice that before steps 500-530, the client does not have the one-time password. These embodiments allow the one-time password to be freely set, to be different for different users, and to be different for multiple user sessions, and the like. Further, someone who was previously given an active one-time password may be prevented from gaining access. Additionally, these embodiments do not require the user to have any token hardware, to pre-register their client system, or to pre-register user data.

Next, in various embodiments the client uses the received one-time password and digitally signs it with the private key to form a digital data packet (a digital signature), step 540. The digital signature and the user's digital certificate are then sent back to the external server, step 560. Accordingly, data from the external server is signed and then returned to the external server.

Appl. No. 09/896,163
Response dated February 2, 2006
Reply to Office Action of November 2, 2005

PATENT

Subsequently, if the digital signature and digital certificate authenticate the user, the one-time password is activated, and the client may use the one-time password to access the protected computer network. Steps 570-690. In various embodiments, if the user is not authenticated and the client attempts to use the one-time password to access the network, the access will be denied. Accordingly, the one-time password in the challenge to the client should be inactive until the user is authenticated.

Certain limitations in the disclosed embodiments are recited in the claims. For example, among other limitations, claim 15, which was un-amended recites: means for receiving a challenge from a verification server via a first secure communications channel, the challenge comprising at least a network password that is inactive; and means for forming a digital signature in response to the network password received from the verification server and to the private key.

II. THE CITED REFERENCES

A. Yatsukawa

Yatsukawa relates to an authentication system where seed values Ds0 used to authenticate a user are initially synchronized.

In Yatsukawa, the client / user sets an initial "seed data" Ds0 for authentication purposes in the client and the server, col. 15, line 66 - col. 16, line 12. From Ds0, Dn-1 are subsequently independently generated on the client and the server. In operation, Yatsukawa describes that the client logs into a server, col. 16, lines 46-52. Next, the server sends an authentication-data request, col. 16, lines 54-55. Then, the client generates authentication data D by enciphering the seed data Dn-1(Ds0) stored at the client by the client private key K, and then authentication data D is sent to the server, col. 16, lines 57-60. The server deciphers the authentication data D using the client public key K to recover the client seed data, col. 17, lines 1-14. Next, the server compares the recovered client seed data to the initial seed data, Ds0, previously provided by the user and stored at the server, col. 17, lines 14-17. As illustrated in Fig. 13, block S5, if the recovered client seed data matches Ds0, access is granted.

Appl. No. 09/896,163

PATENT

Response dated February 2, 2006

Reply to Office Action of November 2, 2005

The Office Action cites col. 12, lines 39-67 as disclosing "A computer program product for a client computing system including a processor" and "wherein the authentication server activates the password that is inactive when the digital signature is verified." The undersigned traverses this assertion. In the cited section, Yatsukawa discloses an authentication terminal apparatus in support of an external authentication server, col. 12, lines 40-44. As discussed previously, the client logs into the server, col. 16, lines 46-52. Next, the server sends the authentication-data request to the client, col. 16, lines 54-55. Then, the client generates authentication data D by enciphering the seed data Ds0 stored at the client (e.g., in the storage medium) by the client private key K, and then authentication data D is sent to the server, col. 16, lines 57-60. In Yatsukawa, Ds0 determined in the authentication server is not inactive and then activated, but once determined as previously discussed, is always active. Nowhere in Yatsukawa is there any mention that the server activates the password.

A major disadvantage of the system is if any authorized user in possession of the initial seed data Ds0, but later becomes unauthorized (e.g., fired), in Yatsukawa, because the user has Ds0, the user can generate a valid password with the software or token card and gain access to the system. In Yatsukawa, Ds0 is not inactive and then activated, but is a seed value that once pre-synchronized by the user with the client and the server, allows the user to generate passwords and authenticate.

Further, the Office Action cites col. 20, lines 11-31 and col. 19, line 7 through col. 20, line 14 as disclosing "A computer program product for a client computing system including a processor includes...code that directs the processor to form a digital signature in response to the password that is inactive from the authentication server and to the private key." The undersigned traverse this assertion. In Yatsukawa, as discusses above, the initial seed data Ds0 is pre-synchronized with the client and the server and nowhere in Yatsukawa does Ds0 get sent to the client from the server, col. 15, line 66 - col. 16, line 12. Importantly, Ds0, which is provided by the client (or token), is digitally signed and provided to the server, col. 20, lines 11-31 and col. 19, line 7 through col. 20, line 14. Additionally, in Yatsukawa, the authentication data request

Appl. No. 09/896,163
Response dated February 2, 2006
Reply to Office Action of November 2, 2005

PATENT

message does not include "a password that is inactive," because the initial seed data Ds0 is pre-synchronized and stored at the client (or token) and the server, see FIG. 13.

B. Chang

Chang relates to a token caching security system.

As previously discussed, Chang states that the function of the Token card is that it "generates a series of random one-time passwords (OTPs)," col. 2, lines 15-16. This user-entered OTP is then compared to an OTP independently generated in a password server. In Chang, the OTP generated by the password server is not ever provided to the user. Instead, the user provides the OTP generated by the Token card to the password server. Nowhere in Chang is there any mention of the OTP being provided to the user from any source other than the Token card.

Further, the Office Action recites "inactive passwords being contained within the request message to an authentication server is a known technique with the use of one-time or temporary passwords" and cites col. 7, lines 21-29. The undersigned traverses this assertion. In the cited section in Chang, the OTP password is independently generated in the Token card, as well as the AAA server. There is nothing in Chang that discusses activating a password. Additionally, Chang merely states that if the CHAP or PAP password entered by the user is correct, the session may be established, col. 7, lines 21-29.

Similar to above, a major disadvantage of the system is if any authorized user in possession of the initial seed data Ds0, but later becomes unauthorized, in Chang, because the user has Ds0, the user can generate a valid password with the software or token card and gain access to the system. In Chang, Ds0 is not inactive and then activated, but is a seed value that once pre-synchronized by the user with the client and the server, allows the user to generate passwords and authenticate.

Appl. No. 09/896,163
Response dated February 2, 2006
Reply to Office Action of November 2, 2005

PATENT

C. Baskey

Baskey was previously discussed as relating to an SSL proxy server, and being silent regarding an authentication protocol.

III. THE CITED REFERENCES DISTINGUISHED

A. Claim 15

The elements of Claim 15 are not disclosed, suggested, or taught by Yatsukawa in view of Baskey or Chang. More specifically the cited references fail to disclose means for receiving a challenge from a verification server via a first secure communications channel, the challenge comprising at least a network password that is inactive.

As discussed above, Yatsukawa is a form of "token-based" authentication where the client determines the authentication-data inspection data. Specifically, Yatsukawa states that the user provides initial seed data Ds0. In Yatsukawa, the challenge from the verification server to the client system does not include "a network password that is inactive," as is recited above. In Yatsukawa, the client must already have Ds0 in memory, and must be pre-synchronized with the server.

Additionally, Baskey is silent as to this limitation, as Baskey simply relates to SSL connections.

The references also fail to disclose means for forming a digital signature in response to the network password received from the verification server and to the private key, and means for communicating the digital certificate and the digital signature to the authentication server.

This limitation is totally missing from Baskey. In Yatsukawa, an initial seed data Ds0 (provided by the user) is digitally signed and provided to the server. In contrast, the digital signature is claimed to be determined in response to the network password that was received

Appl. No. 09/896,163
Response dated February 2, 2006
Reply to Office Action of November 2, 2005

PATENT

from the verification server. Accordingly, what is sent back to the server in Yatsukawa is different from what is recited.

The references also fail to disclose: wherein the network password is activated when the digital signature and the digital certificate authenticate the user. In Yatsukawa, Ds0 determined in the server is not inactive and then activated, but once determined, is always active. Baskey is silent as to this limitation, as Baskey simply relates to SSL connections.

Furthermore, in Chang, the OTP independently determined from the AAA server is not initially inactive. As discussed previously, when the OTP from the Token card matches the OTP independently generated in the AAA server, the user session is initiated. The password determined in the AAA server is not inactive and then activated, but, once determined, is always active.

As discussed in the examples above, in Yatsukawa, a user in possession of Ds0 may log on and be authenticated even if unauthorized. In contrast, by sending inactive passwords, a previously authorized user may not access the system, once the user is fired, for example.

Accordingly, because these cited references fail to disclose at least the above-recited limitations, claim 15 is patentable.

B. Remaining Claims

Claims 1 and 8, are believed to be allowable for at least the same reasons as those given above for claim 15, and more particularly, for the specific limitations they recite, thus the pending rejections are traversed. The Examiner is directed to examine the exact wording of each of these claims.

Claims 2-7, which depend from claim 1 are believed to be allowable for at least the same reasons given above, and more particularly, for the specific limitations they recite, thus the pending rejections are traversed. The Examiner is directed to examine the exact wording of each of these claims.

Appl. No. 09/896,163
Response dated February 2, 2006
Reply to Office Action of November 2, 2005

PATENT

Claims 9-14 and 21 which depend from claim 8 are believed to be allowable for at least the same reasons given above, and more particularly, for the specific limitations they recite, thus the pending rejections are traversed. The Examiner is directed to examine the exact wording of each of these claims.

Claims 16-20, which depend from claim 15 are believed to be allowable for at least the same reasons given above, and more particularly, for the specific limitations they recite. The Examiner is directed to examine the exact wording of each of these claims.

Appl. No. 09/896,163
Response dated February 2, 2006
Reply to Office Action of November 2, 2005

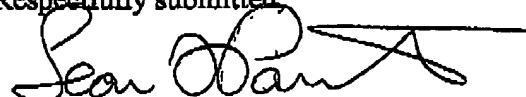
PATENT

CONCLUSION

In view of the foregoing, Applicants believe all claims now pending in this Application are in condition for allowance. The issuance of a formal Notice of Allowance at an early date is respectfully requested.

If the Examiner believes a telephone conference would expedite prosecution of this application, please telephone the undersigned at (650) 326-2400.

Respectfully submitted



Sean F. Parmenter
Reg. No. 53,437

TOWNSEND and TOWNSEND and CREW LLP
Two Embarcadero Center, Eighth Floor
San Francisco, California 94111-3834
Tel: (650) 326-2400
Fax: (650) 326-2422
60691726 v1